Amendment to the Claims:

This listing of claims will replace all versions, and listings, of claims in the application:

1. (Currently Amended) A method of authenticating communication between a first and a second party, the method comprising:

provisioning a ~~first secure credential~~ shared secret between the first party and the second party;

establishing a secure tunnel between the first party and the second party using the ~~first secure credential~~comprising mutually deriving a tunnel key using symmetric cryptography based on the shared secret; and

authenticating a relationship between the first party and the second party within the secure tunnel using ~~a second secure credential to establish an authorization policy; and~~

~~distributing an update to one of the first secure credential and the second secure credential within the secure tunnel to update the authorization policy~~.

2. (Original) The method set forth in claim 1 further comprising the step of protecting the termination of the authenticated conversation by use of a tunnel encryption and authentication to protect against a denial of service by an unauthorized user.

3. (Original) The method set forth in claim 1 wherein the step of provisioning occurs within a wired implementation.

4. (Original) The method set forth in claim 1 wherein the step of provisioning occurs within a wireless implementation.

5. (Currently Amended) The method set forth in claim 1 wherein the ~~first secure credential~~shared secret is a protected access credential (PAC).

6. (Original) The method set forth in claim 5 wherein the protected access credential includes a protected access credential key.

7. (Original) The method set forth in claim 6 wherein the protected access credential key is a strong entropy key.

8. (Original) The method set forth in claim 7 wherein the entropy key is a 32-octet key.

9. (Original) The method set forth in claim 6 wherein the protected access credential includes a protected access credential opaque element.

10. (Original) The method set forth in claim 6 wherein the protected access credential includes a protected access credential information element.

11. (Original) The method set forth in claim 1 wherein the step of provisioning occurs through out-of-band mechanisms.

12. (Original) The method set forth in claim 1 wherein the step of provisioning occurs through in-band mechanisms.

13. (Cancelled)

14. (Currently Amended) The method set forth in claim [[13]]1, wherein the step of establishing a tunnel key further includes the step of establishing a session_key_seed ~~to be used in protecting the secure tunnel integrity and establishing~~ deriving a master session key used for authenticating the relationship.

15. (Original) The method set forth in claim 1 wherein the step of authenticating is performed using EAP-GTC.

16. (Original) The method set forth in claim 1 wherein the step of authenticating is performed using Microsoft MS-CHAP v2.

17. (Currently Amended) A system for communicating via a network, the system comprising:

means for providing a communication link between a first party and a second party;

means for provisioning a ~~first secure credential~~shared secret between the first and the second party;

means for establishing a secure tunnel utilizing the ~~first secure credential~~shared credential, the means for establishing comprises means for deriving a tunnel key using symmetric cryptography based on the shared secret; and

means for authenticating a relationship between the first party and the second party within the secure tunnel ~~using a second secure credential to establish an authorization policy; and~~

~~means for delivering an update to one of the first secure credential and the second secure credential to update the authorization policy~~.

18. (Original) The system for communicating set forth in claim 17 wherein the communication link is a wireless network.

19. (Original) The system for communicating set forth in claim 17 wherein the communication link is a wired network.

20. (Original) The system for communicating set forth in claim 17 wherein the first secure credential is a protected access credential (PAC).

21. (Original) The system for communicating set forth in claim 18 wherein the wireless network is an 802.11 wireless network.

Claims 22 -23 (Cancelled)

24. (New) A wireless device, comprising:

the wireless client is configured to receive a shared secret between the wireless client and a second wireless device;

the wireless client is configured to establish a secure tunnel between the first wireless device and the second wireless device using the shared secret to mutually derive a tunnel key using symmetric cryptography based on the shared secret; and

the wireless client is configured to mutually authenticate with the second wireless device employing the secure tunnel.

25. (New) A wireless device according to claim 24, the wireless client is configured to receive a shared secret further comprising establishing a second secure tunnel for receiving the shared secret.

26. (New) A wireless device according to claim 24, the wireless device is configured to establish a secure tunnel further comprises establishing a session key seed for deriving a master session key used for mutually authenticating the second wireless device employing the secure tunnel.